Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

GDPR AS GLOBAL STANDARD SETTER SYMPOSIUM

The charm of jurisdictions: a modern version of Solomon's judgment?

STEPHAN KOLOSSA — 5 June, 2019

From a perspective of international law, the General Data Protection Regulation (GDPR) pioneers particularly in terms of its (extraterritorial) application. Whereas in international law, which is based on the Westphalian notion of exclusive state sovereignty, this sovereignty is usually restricted to the state's own territory and allows for an extraterritorial application of human rights only in exceptional circumstances, the GDPR prominently standardises the domestic-market principle in Article 3(2) GDPR. The principle imposes obligations on processors or controllers that are based outside of the European Union (EU), given that they offer goods or services to people inside the EU or monitor the behaviour of people within the EU. This brings up an important question: Does Art. 3 (2) GDPR indicate a structural shift towards more expansive exercise of jurisdiction in cyberspace? Such a shift could have ramifications for the regulation of cyberspace well beyond data protection law: While the discussions around jurisdiction in cyberspace have still not come to a broad consensus, international human rights law might be able to learn from data protection law how to protect and safeguard human rights online.

The Snowden revelations have shown a glimpse of the global surveillance apparatus and have also triggered many debates about the protection of the rights to privacy online and their limits as to the scope of the various treaty regimes. Focusing on the international right to privacy and the right to data protection, it may not be far-fetched to allow for a broader exercise of jurisdiction in the digital era.

The default rule in international law: No extraterritorial jurisdiction

The principles of jurisdiction in public international law as well as international relations are of fundamental importance: They concern the allocation between states and other entities, such as the EU, of the competence to regulate daily life. It includes the competence of a state to secure the differences that make each state a distinct society. Equally, the state may define its coercive powers. Jurisdiction is closely linked to the sovereign equality and territorial sovereignty of states (cf. Art. 2 (1) Charter of the United Nations [UNC]). Already the Permanent Court of International Justice (PCIJ) held in its famous *Lotus* case:

> ***"the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule of the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention"***
>
> **(PCIJ, „Lotus", Judgment No. 9, 1927, Ser. A, No 10, pp. 18-19).**

Therefore, the default rule in international law is that a state cannot exercise jurisdiction with extraterritorial effects unless there is a permissive rule to the contrary.

Jurisdiction also applies in cyberspace

As public international law is traditionally state-centric, the question

has been given new attention as to the continuously emerging importance of the cyberspace and the state's role within it. During the early times of the Internet as we know it today, cyberspace has often been regarded as a separate, de-territorialized space. Most prominently John Perry Barlow has called for the cyberspace to be independent from state interference. Today it has become evident that even though cyberspace is largely run by private entities, states do play important roles in the way it functions. Governments can block traffic and largely intercept communication. Given that the physical infrastructure of cyberspace is built upon a state's territory, cyberspace is not immune from national jurisdiction. Moreover, attempts to categorize cyberspace as a *global common*, such as outer space and the high seas, has proven equally difficult as cyberspace is man-made, fully intangible, highly changeable, and the exploitation of data does not lead to its destruction. Hence, although cyberspace has a sui generis character it is not autonomous from the exercise of a state's jurisdiction.

Yet, it remains the question on which basis a state (or in the case of the EU a supranational organization) can exercise jurisdiction in cyberspace. In general, the principles of territoriality and personality are the main bases of international law. As for the applicability in cyberspace it appears natural to stipulate national jurisdiction for a situation with a nexus to the domestic territory. If *e.g.* data is stored on a server located within a state, this state exercises jurisdiction over the server and the stored data. For the personality principle, it becomes somewhat less simple. The active personality principle does not pose too many problems. A company based in the EU processing personal data outside of the EU is still bound by the GDPR, regardless of where it processes the data (Art. 3 (1) GDPR). The passive personality principle proves to be more complicated. In the context of the GDPR it means that any company offering services to a person in the EU must abide by the GDPR even if it has no other "nexus" to the EU. Although this might be beneficial from an EU point of view, it imposes obligations on companies which simultaneously are obliged to comply with the law of the territorial state in which they operate. Hence, the passive personality principle produces extraterritorial effects. Remembering the PCIJ dictum in the Lotus case this brings up the question: Is a

permissive rule emerging which allows for the exercise of jurisdiction based on the passive personality principle?

The passive personality principle as a basis for jurisdiction in international law

Exercising jurisdiction based on the passive personality principle is not a new phenomenon in international law. It has been applied in singular circumstances such as against a US citizen by Mexico already in 1885 who was based in the USA and alleged of libelling a Mexican national in a US newspaper. Simply because the victim was Mexican, Mexico assumed jurisdiction over the perpetrator. The USA denied any jurisdiction for Mexico. However, recently there might have been a trend in international law in favour of accepting the type of passive personality jurisdiction. One of the Separate Opinions in the *Arrest Warrant* case noted that at least for some kind of criminal offenses the passive personality principle seems to meet little opposition nowadays. On the other side, one should be careful to simply derive a general acceptance from several instances of criminal law cases and more precisely to cases that concerned the prosecution of terrorism. Especially when analyzing jurisprudence in the field of international human rights law it is doubtful whether the principle equally applies more generally. The European Court of Human Rights (ECtHR) for instance has pointed out that the European Convention on Human Rights and Fundamental Freedoms (ECHR) generally does not govern the actions of states which are not parties to it; neither based on some kind of effects for nationals of a member state nor on the classical passive personality principle. More specifically it has found that the mere publishing of a person's information does not constitute the necessary nexus that would suffice for a jurisdiction. Hence, it is not yet clear if the exercise of jurisdiction based on the passive personality principle in the GDPR is indicative of a broader trend towards the acceptance of the exercise of such jurisdiction in other areas of international law.

How to resolve jurisdictional conflicts: Insights from other areas of international law

The reason against any broadening of a state's jurisdiction beyond its

national borders is evident — a state seeking to expand jurisdictional power hereby restricts the jurisdiction of other states. Instances of overlapping or concurrent jurisdiction are not welcome. If such situations indeed occur, the question arises as to the priority of one state's jurisdiction. Existing possible answers constitute blocking statutes such as the European Council Resolution 2271/96. Blocking statutes may be an answer, but they are, however, no solution to the problem. Another proposal (often adopted by US courts) tries to balance the interests at stake: the interest of applying the domestic law vs. the interest of not applying it. A more convincing solution may be found in international economic law. One example is the antitrust cooperation procedure established by the European Community and the USA (EC-US Agreement on the Application of Positive Comity Principles in the Enforcement of their Competition Laws).

So far, in terms of conflicting cyber jurisdictions there is no perfect solution yet. Nevertheless, such solution must ensure the right of every state to safeguard the right to protect its own sovereignty without violating the sovereignty of another state. And more importantly, it should be found fast.

Is data protection law the answer?

It is interesting that the GDPR in the name of protecting the right to data protection boldly establishes the domestic-market principle thereby exactly including mere effects on EU citizens regardless of the location or nationality of the data controller. One must be careful when determining the current international legal status of such rules. The State of California already applies such approach, given that there does not exist a federal data protection law. Correspondingly, other new data protection rules apply the same standard, such as the Brazilian General Data Protection Law that will enter into force in 2020. As long as the level of data protection remains similar, potential jurisdictional conflicts between data protection laws will most likely remain resolvable in practice. However, disputes will arise in situations when the material laws differ from one another. So far, states seem to claim as much jurisdictional space as they can get. Material clashes of laws are likely to appear sooner or later that could lead to undesired legal uncertainties. In a practical way, a solution could be sought in

escaping to the rules of enforcement of the GDPR, as enforcement jurisdiction is generally regarded as strictly limited to the territory. Yet, this way one would *de facto* ignore the actual legal problem at hand. The establishment of cooperation mechanisms as mentioned above will most likely fail due to political differences. The most probable solution will be a sovereignty-friendly, thus restrictive interpretation of Article 3(2) GDPR. A glimpse of a possible fix might show the case of Google Inc. v. CNIL (Case C-507/17), currently pending before the European Court of Justice. EU Advocate General Szpunar has recently expressed in his opinion, that the territorial scope of the right to be forgotten should be limited to the EU, thereby denying extra-territorial applicability. The final decision to the case will not solve all of the issues with regard to scope of the GDPR. But it will certainly assist in the search for a wise "Solomonic" decision, and show whether Europe is indeed the "true" mother of data protection.

*Stephan Kolo*ß*a is PhD candidate at the Institute for International Law of Peace and Armed Conflict – Ruhr University Bochum. As a member of the transdisciplinary research group SecHuman, his research focuses on security for people in cyberspace, specifically the right to privacy.*

Cite as: Stephan Koloß**a, "The charm of jurisdictions: a modern version of Solomon's judgment?", *Völkerrechtsblog*, 5 June 2019, doi: 10.17176/20190611-164341-0.**

ISSN 2510-2567

Tags: *Cyber*, *Data Protection*, *European Union*, *Jurisdiction*

Related

One law to rule them all
5 February, 2018
In "Discussion"

Designed to serve mankind?
27 May, 2019

The internet on its way back to a future of human dignity?

In "GDPR as Global Standard Setter"

29 May, 2019
In "GDPR as Global Standard Setter"

PREVIOUS POST
The GDPR and algorithmic decision-making

NEXT POST
Centenary struggles: climate change & informality at ILO 100

No Comment

Leave a reply

Your email address will not be published. Required fields are marked *

Name (required)

E-Mail (required)

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.